Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF

Jean Goubault-Larrecq

ANR Blanc CPP

PLC Festschrift – Sep. 2013

Outline

Outline

PCF, Full Abstraction

PCF [Plotkin77]:

- a call-by-name, simply-typed, higher-order functional language
- no side-effects
- has computational adequacy
- fails full abstraction. . . except with additional `por`

PCF, Full Abstraction

PCF [Plotkin77]:

- a call-by-name, simply-typed, higher-order functional language
- no side-effects
- has computational adequacy
- fails full abstraction. . . except with additional `por`

Here, PCF plus specific choice effects:

- Will concentrate on angelic non-deterministic choice
- also probabilistic choice, + mixed

Outline

Types

$$
\begin{array}{rcll}
\gamma & ::= & \mathtt{Nat} \mid \mathtt{S} & \text{Ground types} \\
\sigma, \tau & ::= & \gamma \mid \sigma \to \tau \mid \mathtt{T}\tau & \text{Types}
\end{array}
$$

Notes:

- $\mathtt{S}$ has only one (non-bottom) value
  $=$ `unit` type, termination type

  Not required in principle, but practical

- $\mathtt{T}\tau$ type of processes computing value of type τ

  à la [Moggi91]

PCF(S) Terms

Language parameterized by set $S \subseteq \{\mathtt{A}, \mathtt{D}, \mathtt{P}\}$
(angelic non-det., demonic non-det., probabilistic choice).

- PCF terms
  (λ-calculus + basic arithmetic + $\mathtt{ifz}$ + fixpoint Y)
- At $\mathtt{S}$ type:
  - $\top : \mathtt{S}$
  - for every $M : \mathtt{Nat}$, $\mathtt{ignore}\, M : \mathtt{S}$
  - for all $M : \mathtt{S}$, $N : \sigma$, sequencing $M; N : \sigma$
- At $\mathtt{T}\tau$ types:
  - for each $M : \tau$, $\mathtt{val}\, M : \mathtt{T}\tau$
  - for all $M : \sigma$, $N : \mathtt{T}\tau$, $\mathtt{let}\, x \Leftarrow M \,\mathtt{in}\, N : \mathtt{T}\tau$
  - Non-det. choice $\bigcirc\!\!\!\!\vee : \mathtt{T}\tau \to \mathtt{T}\tau \to \mathtt{T}\tau$
  - Prob. choice $\oplus : \mathtt{T}\tau \to \mathtt{T}\tau \to \mathtt{T}\tau$

Operational Semantics

Use judgments $E \cdot M \downarrow^{\text{may}} a$, $a \in \mathbb{Q} \cap [0,1]$.

"The probability that $E \cdot M$ may terminate is $> a$"

- Redex discovery/computation rule $C \to C'$:

$$\frac{C' \downarrow^m a}{C \downarrow^m a} \qquad \text{for each rule } C \to C' : \quad \begin{array}{l} E \cdot MN \to E[\_N] \cdot M \\ E[\_N] \cdot \lambda x \cdot P \to E \cdot P[x := N] \text{ etc.} \end{array}$$

- Final state $\mathtt{val}\ \_ \cdot \underline{\top}$:

$$\frac{}{\mathtt{val}\ \_ \cdot \underline{\top} \downarrow^m a} \ (a \in \mathbb{Q} \cap [0,1))$$

- Choice:

$$\frac{E \cdot M \downarrow^{\text{may}} a}{E[\_MN] \cdot \textcircled{\vee} \downarrow^{\text{may}} a} \quad \frac{E \cdot N \downarrow^{\text{may}} a}{E[\_MN] \cdot \textcircled{\vee} \downarrow^{\text{may}} a} \quad \frac{E \cdot M \downarrow^{\text{may}} a \quad E \cdot N \downarrow^{\text{may}} b}{E[\_MN] \cdot \oplus \downarrow^{\text{may}} \frac{1}{2}(a+b)} \ (\oplus)$$

Termination Semantics

Definition

$\mathrm{Pr}(E \cdot M{\downarrow}^{\mathsf{may}}) = \sup\{a \in \mathbb{Q} \in [0,1] \mid E \cdot M \downarrow^{\mathsf{may}} a \text{ derivable}\}$

- $\mathrm{Pr}(\mathtt{val}\,\_ \cdot \underline{\top}{\downarrow}^{\mathsf{may}}) = 1$
- $\mathrm{Pr}(E[\_MN] \cdot \oplus{\downarrow}^{\mathsf{may}}) = \frac{1}{2}(\mathrm{Pr}(E \cdot M{\downarrow}^{\mathsf{may}}) + \mathrm{Pr}(E \cdot N{\downarrow}^{\mathsf{may}}))$
- $\mathrm{Pr}(E[\_MN] \cdot \oslash{\downarrow}^{\mathsf{may}}) = \max(\mathrm{Pr}(E \cdot M{\downarrow}^{\mathsf{may}}), \mathrm{Pr}(E \cdot N{\downarrow}^{\mathsf{may}}))$

Denotational Semantics: Previsions

Let $[\![\mathrm{T}\tau]\!]_S$ as spaces of previsions over $[\![\tau]\!]_S$ [JGL-CSL07]

Definition (Prevision on X)

Let $I = [0,1]$, as a dcpo. A Scott-continuous functional $F : [X \to I] \to I$ is a prevision iff:

- $F(ah) = aF(h)$ for every $a \in I$
- $F(\frac{a+h}{2}) = \frac{1}{2}(a + F(h))$ (total mass $= 1$)
- $F(\frac{h+h'}{2}) \leq \frac{1}{2}(F(h) + F(h'))$
- $F(h) \in \{0,1\}$ for every $h : X \to \{0,1\}$ (if $\mathrm{P} \notin S$)

Note: by representation theorems [JGL08], match the usual Hoare/Smyth powerdomains, as well as [MOW03, TKP05].

Denotational Semantics

$$[\![\lambda x \cdot M]\!]_S = (x \mapsto [\![M]\!]_S) \qquad [\![MN]\!]_S\,(\rho) = [\![M]\!]_S\,([\![N]\!]_S)$$

$$\begin{array}{rcl}
[\![Y]\!]_S & = & (f \mapsto \bigcup_{n\in\mathbb{N}} f^n(\bot)) \\
[\![\mathtt{val}\, M : \mathrm{T}\sigma]\!]_S & = & (h \mapsto h([\![M]\!]_S)) \\
[\![\mathtt{let}\, x \Leftarrow M \,\mathtt{in}\, N]\!]_S & = & (h \mapsto [\![M]\!]_S\,(x \mapsto [\![N]\!]_S\,(h)) \\
[\![\bigcirc\!\!\!\!\vee]\!]_S & = & (F_1, F_2, h \mapsto \max(F_1(h), F_2(h)) \\
[\![\oplus]\!]_S & = & (F_1, F_2, h \mapsto \frac{1}{2}(F_1(h) + F_2(h))(\text{if } \mathtt{P} \in S)
\end{array}$$

Soundness

In usual PCF, soundness states that if $M \to^* V$ then $[\![M]\!] = [\![V]\!]$.

Theorem (Soundness)

Let $\blacklozenge = \chi_{\{\top\}} : [\![\mathbb{S}]\!] \to I$ *map* $\bot$ *to* 0, $\top$ *to* 1 *(termination-observing continuation).*

- *If* $E \cdot M \downarrow^{\text{may}} a$ *then* $[\![E[M]]\!]_S(\blacklozenge) > a$

Proof: induction. □

Corollary

- $[\![E[M]]\!]_S(\blacklozenge) \geq \Pr(E \cdot M{\downarrow}^{\text{may}})$

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S\,(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\text{may}})$

Proof: The key point is the definition of a suitable logical relation... and precisely there is a general definition of...

Under consideration for publication in Math. Struct. in Comp. Science

Logical Relations for Monadic Types†

JEAN GOUBAULT-LARRECQ[1‡]
and SŁAWOMIR LASOTA[1,2§]
and DAVID NOWAK[1¶]

[1] *LSV/CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan, 61, avenue du président-Wilson, 94235 Cachan Cedex, France*

[2] *Institute of Informatics, Warsaw University, ul. Banacha 2, 02-097 Warszawa, Poland*

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S\,(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{may}})$

Proof: The key point is the definition of a suitable logical relation...
and precisely there is a general definition of...

Under consideration for publication in Math. Struct. in Comp. Science

Logical Relations for Monadic Types†

JEAN GOUBAULT-LARRECQ[1‡]
and SŁAWOMIR LASOTA[1,2§]
and DAVID NOWAK[1¶]

[1] *LSV/CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan, 61, avenue du président-Wilson, 94235 Cachan Cedex, France*

[2] *Institute of Informatics, Warsaw University, ul. Banacha 2, 02-097 Warszawa, Poland*

which is absolutely
not
what we need

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\text{may}})$

Proof: Define a logical relation R_σ by (something like) double orthogonality:

$$M \, R_{\mathrm{T}\sigma} \, F \quad \text{iff} \quad \text{for all } E \, R_\sigma^\perp \, h, \ \Pr(E \cdot M{\downarrow}^m) \geq F(h)$$

$$E \, R_\sigma^\perp \, h \quad \text{iff} \quad \text{for all } Q \, R_\sigma \, v, \ \Pr(E \cdot \mathtt{val}\ Q{\downarrow}^m) \geq h(v)$$

Then do some stuff and conclude. □

Outline

Full Abstraction

Let $M \precsim^{\text{may}} N$ iff $\Pr(E \cdot M{\downarrow}^{\text{may}}) \leq \Pr(E \cdot N{\downarrow}^{\text{may}})$ for every $E : \tau \vdash \mathtt{TS}$.

Conjecture (Full Abstraction)

$M \precsim^{\text{may}} N$ iff $[\![M]\!]_S \leq [\![N]\!]_S$, at all types.

- Easy direction: If $[\![M]\!]_S \leq [\![N]\!]_S$ at type τ, then $[\![E[M]]\!]_S \leq [\![E[N]]\!]_S$ for every context $E : \tau \vdash \mathtt{TS}$
  So $\Pr(E \cdot M{\downarrow}^{\text{may}}) \leq \Pr(E \cdot N{\downarrow}^{\text{may}})$ by computational adequacy.

- Hard direction: assume $[\![M]\!]_S \not\leq [\![N]\!]_S$, find E such that $\Pr(E \cdot M{\downarrow}^{\text{may}}) > \Pr(E \cdot N{\downarrow}^{\text{may}})$
- So hard that it is wrong for PCF...
  but true for PCF($\mathtt{A}$)!

Definability

Pierre-Louis has always told us that definability was the key to full abstraction.

Definability and full abstraction

Pierre-Louis Curien[1]

PPS, CNRS and University Paris 7

Abstract

Game semantics has renewed denotational semantics. It offers among other things an attractive classification of programming features, and has brought a bunch of new definability results. In parallel, in the denotational semantics of proof theory, several full completeness results have been shown since the early nineties. In this note, we review the relation between definability and full abstraction, and we put a few old and recent results of this kind in perspective.

Keywords: operational semantics, denotational semantics, sequentiality.

Definability. . . of Opens

So assume $[\![M]\!]_S \not\leq [\![N]\!]_S$, of type τ.

- Since $\leq$ is specialization ordering of (Scott) topology, there is a separating open set U:

$$[\![M]\!]_S \in U \qquad [\![N]\!]_S \notin U$$

- If we can define U by a context E, then:

$$[\![E[M]]\!]_S = \top \qquad [\![E[N]]\!]_S = \bot$$

  so by computational adequacy

$$\Pr(\mathtt{val}\ E \cdot M{\downarrow}^{\mathsf{may}}) = 1 > 0 = \Pr(\mathtt{val}\ E \cdot N{\downarrow}^{\mathsf{may}})$$

  So $M \not\precsim^{\mathsf{may}} N$.

- By contraposition, $M \precsim^{\mathsf{may}} N$ implies $[\![M]\!]_S \leq [\![N]\!]_S$. So full abstraction will hold.

Definability... of Subbasic Opens

So assume $[\![M]\!]_S \not\leq [\![N]\!]_S$, of type τ.

- Since $\leq$ is specialization ordering of (Scott) topology, there is a separating open set U in a given subbase $\mathcal{B}_\tau$:

$$[\![M]\!]_S \in U \qquad [\![N]\!]_S \notin U$$

- If we can define U by a context E, then:

$$[\![E[M]]\!]_S = \top \qquad [\![E[N]]\!]_S = \bot$$

  so by computational adequacy

$$\Pr(\mathtt{val}\, E \cdot M{\downarrow}^{\mathsf{may}}) = 1 > 0 = \Pr(\mathtt{val}\, E \cdot N{\downarrow}^{\mathsf{may}})$$

  So $M \not\precsim^{\mathsf{may}} N$.

- By contraposition, $M \precsim^{\mathsf{may}} N$ implies $[\![M]\!]_S \leq [\![N]\!]_S$. So full abstraction will hold.

Choosing the Right Subbase

Fortunately:

Lemma

For every type τ, $[\![\tau]\!]_S$ is a bc-domain.

(One of the nice CCCs of continuous domains.)

Proposition (Key result — *coincidence of topologies*)

If X and Y are bc-domains, then:

- *Scott topology on $[X \to Y]$ = pointwise convergence*
  Subbasis: $[a \in V] = \{f \mid f(a) \in V\}$, $a \in X$, V open in Y
- *Scott topology on previsions on X = weak topology*
  Subbasis: $[h > r] = \{F \mid F(h) > r\}$, $h \in [X \to I]$, $r \in \mathbb{Q}$

Definability of Subbasic Opens

Miracle

All these subbasic opens are *definable*.

- E.g., on $[X \to Y]$,
  Let a be defined by term t
  Let V be defined by context E
  Then $[a \in V]$ is defined by context $E[\_t]$.

Mission accomplished!

. . . almost.
We actually need to define elements a as well.
Eventually, this requires some additional constructions.
E.g., sup of maps requires $\bigcirc\!\!\!\!\vee$ (non-det. choice).
Worse: prob. choice $\oplus$ requires statistical termination testers.

The Purely Angelic Case

Without probabilities, $M \precsim^{\mathsf{may}} N$ simplifies to:
for every context E, $E \cdot M{\downarrow}^{\mathsf{may}}$ implies $E \cdot N{\downarrow}^{\mathsf{may}}$.

Theorem (Case $S = \{\mathtt{A}\}$)

Full abstraction holds for PCF($\{\mathtt{A}\}$):

$$M \precsim^{\mathsf{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A}\}} \leq [\![N]\!]_{\{\mathtt{A}\}}$$

Note 1: No need for parallel or . . . which is in fact definable: $M \ \mathtt{por}\ N = (M \mid\mid N) \circledS (N \mid\mid M)$
Note 2: Proof much simpler than Plotkin's for PCF+por. . . but language is different.

Note 3: Implies full abstraction for (isomorphic) semantics using Hoare powerdomains instead of previsions.

The Angelic+Probabilistic Case

We now need termination testers $\mathtt{Pr}(M > b)$ to the language $(M : \mathtt{TS})$

$$\frac{\_ \cdot M \downarrow^{\text{may}} b \quad E \cdot \top \downarrow^{\text{may}} a}{E \cdot \mathtt{Pr}(M > b) \downarrow^{\text{may}} a} (\mathtt{Pr}) \quad [\![\mathtt{Pr}(M > b)]\!]_S = \begin{cases} \top & \text{if } [\![M]\!]_S (\blacklozenge) > b \\ \bot & \text{otherwise} \end{cases}$$

The Angelic+Probabilistic Case

Let $M \lesssim^m N$ iff $\Pr(\_ \cdot E'[M]{\downarrow}^m) \leq \Pr(\_ \cdot E'[N]{\downarrow}^m)$
for every extended context E' $\qquad E' ::= \ldots \mid \Pr(\_ > b)$

Theorem (Case $S = \{\mathtt{A}, \mathtt{P}\}$)

Full abstraction holds for PCF($\{\mathtt{A}, \mathtt{P}\}$) + statistical testers:

$$M \lesssim^{\text{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{P}\}}$$

Proof. As before, there is a subbasis of definable opens. □

Outline

Conclusion

The angelic cases . . . are angelic:

- PCF({A}) is fully abstract
- PCF({A, P}) is fully abstract
  provided we add statistical termination testers
- I cheated a bit: we need a bit of call-by-value to define the probabilistic contexts
- Demonic/erratic cases slightly more difficult
- Purely probabilistic case hopeless
  unless we turn to random variables, maybe.